The Security Page

IDENTITY THEFT-WHO CAN BE A VICTIM?

How would you feel if you were stopped for a traffic violation and suddenly found yourself being handcuffed and taken to jail for a crime you never committed? Or if you got a nasty call from a collection agency for a car loan you never had? Or if your application for a home mortgage was turned down because of information in your credit report about overdue bills on accounts you never opened? These are situations you could face as a victim of identity theft. While ID theft can take many complex forms, the essence of this crime is simple-someone steals personal information about you to use for fraudulent purposes. ID theft can happen to anyone. By guarding your personal information carefully, you can reduce the likelihood of becoming a victim. But you may not be able to avoid ID theft entirely; it can happen in ways beyond your control. Businesses, government agencies, and organizations that obtain personal information also have a responsibility to handle it carefully and keep it secure.

One of the scariest things about ID theft is that it can happen anywhere your personal information is kept. Your life is filled with potential crime scenes. Your mailbox, employer's files, doctor's office, computer, and even your back pocket are all vulnerable to criminals who want to get your personal information and use it to their advantage. Here are some common scenarios of ID theft-where it can happen and the harm that can follow, depending on what's been stolen.
Your personal information is a gold mine for ID thieves. Look at each item below to see what might happen if an ID thief got his or her hands on it. Review the following scenarios and think of how many times a week you use this information:

- Your wallet or purse, containing your credit and debit cards, social security number and checks is stolen from you at work, at a restaurant, on the subway, or someplace else.

- Someone breaks into your home and steals your ATM Card and the PIN number that you wrote on a note in your desk.

- Your incoming or outgoing mail, including bills, bank statements and checks you have written, and pre-approved credit card offers is stolen from your mailbox.

- "Dumpster divers" steal receipts for transactions you made with your credit and debit cards from the trash container behind a business or at your home.

- At the airport, someone looking over your shoulder as you dial from a pay phone memorizes your calling card number.

- An information service on the Internet sells your name, address and social security number to someone who has a fraudulent motive for buying it.

- A computer hacker gets into the personal computer databases and steals your name and address and the account numbers of your credit and debit cards.

- Someone uses your personal identification to call your bank and access your bank account information.

- Someone calls or emails you pretending to be with your bank, Internet service provider, or another company you do business with and asks to "verify" your bank account information or the password for your account.

- Someone gets your credit report posing as an employer, landlord, or creditor who would have a legitimate right to that information.

These are but a few examples of the many scams that are on-going in daily life. Here's what can happen if that information gets in the wrong hands:

ATM Card
If someone has both your ATM card and your PIN number, they can withdraw money from your account or use it to make purchases at stores, gas stations, and other places.

Bank Account Information
With your bank account and routing number, someone may be able to create fake checks in your name or, posing as a legitimate merchant, withdraw money from your account for a purchase that you never made.

Bills
Your bills may contain all sorts of information - your name, address, telephone number, bank account, credit and debit card numbers, even your social security number if it's used by the business to identify your account. That information can be used to take over your accounts, to open new accounts in your name, and for other purposes.

Calling Card
With your calling card number (and PIN, if there is one) crooks can make long distance calls to anywhere in the world on your dime.

Checks

Store clerks can't tell that a check is forged, so it's easy to use stolen checks to make purchases. Most banks won't cash checks for people unless they are customers, but there are many check cashing outlets that thieves may be able to use.

Credit and Debit Cards
Many stores don't ask for identification or compare the signature on the back of your card with your receipt. That makes it relatively easy for thieves to use them to make purchases at stores, on the Internet, over the phone, or by mail. It isn't necessary to have the physical card to make long-distance purchases - all the thief needs is your name and account number. The thief can arrange for the goods to be delivered to a different address. If fraudulent merchants have your credit or debit card account numbers, they can charge or debit you for purchases you never agreed to make.

Credit Report
Your credit report lists many of the accounts that you have with businesses. It contains your social security number (full or partial) and information about where you live, where you bank, and where you work. If this information falls into the wrong hands, it can be used to take over your accounts, open new accounts in your name, and impersonate you for many other purposes.

Name and Address
Your name and address by themselves aren't very useful to ID thieves, but they may be the foundation for fraud when combined with other information that may be available from public records and other sources.

Passwords
The passwords that you use to go online and for various online accounts enable thieves to use your accounts to send messages and computer viruses in your name, pose as you to buy or sell things, and get access to online banking accounts and other sensitive information.

Personnel Records
Records about you at work contain your name, address, social security number, and your bank account information if your pay is directly deposited. They may also have information about family members. This information can be used to impersonate you for many fraudulent purposes.

Pre-approved Credit Card Offers
Crooks can apply for new credit card accounts using preauthorized offers of credit originally sent to you. They change the address so the cards will come to them.

Social Security Numbers
Your social security number is the key to your identity and can be used to impersonate you in order to open new credit accounts in your name, get your credit report, apply for government benefits, get a job, open a bank account, rent an apartment, obtain a drivers license, get utility service, and secure a loan. It can even be used to get a marriage license, file bankruptcy, and pay taxes in your name. If someone using your identity is charged with a crime, you could be arrested.

Shred Your Personal Information
Personal sized shredders are available at many major stores at very affordable prices. When selecting a shredder, buy a "cross-cut" style that shreds the information in very small pieces. You are also authorized and even encouraged to deposit your personal unwanted and no longer needed information and mail in the SHRED-IT containers located throughout our facilities. This information will not leave the facility until it is completely decimated and unusable.

For Victims: What to Do

It's frightening to lose your wallet or discover that someone has used information about you for a fraudulent purpose. Don't panic-help is available. You will need to remain calm, cool, and collected as you go through the process of resolving the problem

Know that ID theft is a crime
The federal government and many states have enacted specific laws against ID theft.

Report ID theft to the three major credit bureaus
They will put a "fraud alert" on your credit file so that if someone is applying for credit using your personal information, the creditor will take extra care to ensure that it's really you. They will also send you a free copy of your report so you can check for any accounts that you didn't open.

Report ID theft to law enforcement agencies.
It isn't always possible for the police to investigate every individual case of ID theft, but making an official report can help you as you fight to clear your name, and the information you provide may be used to stop the thief from victimizing others. If you know where the theft occurred, contact the police in that city or town; otherwise, call your local police. Insist on making a formal police report and request a copy.

When a financial account is involved, contact the bank immediately.
If your credit, card, debit card, ATM card, or checks have been lost or stolen, or if you suspect that someone has obtained your account number for fraudulent

purposes, inform the financial institution promptly and ask what you need to do to protect your money.

Know your payment card rights.
Under federal law, you are not responsible for more than $50 if someone uses your credit card without authorization, and most issuers will remove the charges completely if you report the problem as soon as you discover it. While you could be liable for greater losses if someone uses your debit card, the card issuer may have a policy that offers you more protection than federal law provides.

Contact the Federal Trade Commission's (FTC) ID Theft Hotline.
This toll-free number, 877-438-4338, was established at the direction of Congress to provide a central source of advice for ID theft victims. Victims can also go online at ww.consumer.gov/idtheft to report the problem and get resources to guide them. The information that victims provide is also useful to the FTC and other government agencies in investigating and tracking ID theft. The FTC will send you a comprehensive booklet with step-by-step instructions for how to contact the major credit bureaus and other actions that you may need to take, and forms that you can use to make the process easier.

Should you require further information on this or any other security related matter, contact your security manager.

"Security is Everyone's Business"